



# **Unit Guide to Disaster Recovery Planning Complete**

**Executive Summary:**  
**Unit Guide to Disaster Recovery Planning**

The University has recognized the significance of each unit producing and maintaining Disaster Recovery Plans in order to prepare and address how each unit will continue doing business in the event of a severe disruption or disaster. The Disaster Recovery Planning Team, coordinated by the Client Advocacy Office (CAO) will be the primary resource for assisting each unit with the DRP initiative, by providing education, awareness and tools. The team will work to identify, collect, and organize information and tools for disaster recovery planning and documentation, and disseminate all information to University units in an effective and easily understood manner, so that unit plans may aggressively be developed, tested, distributed, and a copy provided to the CAO for central tracking purposes. After the initial endeavor, the responsibility for providing support will transition from the DRP Team to the Client Advocacy Office.

**Definitions:**

**Business Continuity** is an all-encompassing term covering both disaster recovery planning and business resumption planning. **Disaster Recovery** is the ability to respond to an interruption in services by implementing a plan to restore an organization's critical business functions. Both are differentiated from **Loss Prevention Planning**, which comprises regularly scheduled activities such as system back-ups, system authentication and authorization (security), virus scanning, and system usage monitoring (primarily for capacity indications). The primary focus of this effort is on Disaster Recovery Planning.

**Developing the Plan:**

The following ten steps, more thoroughly described in the document that follows, generally characterize disaster Recovery Plans:

**Phase I – Information Gathering**

1. Organize the Project
2. Conduct Business Impact Analysis
3. Conduct Risk Assessment
4. Develop Recovery Strategy
5. Review Onsite and Offsite Backup and Recovery Procedures
6. Select Alternate Facility

**Phase II – Writing and Testing the Plan**

7. Develop Recovery Plan
8. Test the Plan

**Phase III – Maintaining and Auditing the Plan (Ongoing)**

9. Maintain the Plan
10. Perform Periodic Audit

## Purpose and Scope for a Unit Disaster Recovery Plan

The primary reason for a unit to engage in Disaster Recovery Planning is to ensure the ability of the unit to function effectively in the event of a severe disruption to normal operations. Severe disruptions can arise from several sources: natural disasters (tornadoes, fire, flood, etc.), equipment failures, process failures, from mistakes or errors in judgment, as well as from malicious acts (such as denial of service attacks, hacking, viruses, and arson, among others). While the unit may not be able to prevent any of these from occurring, planning enables the unit to resume essential operations more rapidly than if no plan existed. Before proceeding further, it is important to distinguish between loss prevention planning and disaster recovery planning. The focus of loss prevention planning is on minimizing a unit's exposure to the elements of risk that can threaten normal operations. In the technology realm, unit loss prevention planning includes such activities as providing for system back-ups, making sure that passwords remain confidential and are changed regularly, and for ensuring operating systems remain secure and free of viruses. Disaster recovery planning focuses on the set of actions a unit must take to restore service and normal (or as nearly normal as practical) operations in the event that a significant loss has occurred for critical functions. A systematic disaster recovery plan does not focus unit efforts and planning on each type of possible disruption. Rather it looks for the common elements in any disaster: i.e., loss of information, loss of personnel, loss of equipment, loss of access to information and facilities, and seeks to design the contingency program around all main activities the unit performs. The plan will specify the set of actions for implementation for each activity in the event of any of these disruptions in order for the unit to resume doing business in the minimum amount of time.

Disaster Recovery Planning consists of three principal sets of activities.

1. Identifying the common elements of plausible disruptions that might severely disrupt critical or important unit operations.
2. Anticipating the impacts and effects that might result from these operational disruptions.
3. Developing and documenting contingent responses so that recovery from these interruptions can occur as quickly as possible.

The major outcome of a Unit Disaster Recovery Planning Project is the development of a unit plan. The plan benefits the unit in that it:

- Establishes the criteria and severity of a disruption based on the impact the disruption will cause to the unit's critical functions.
- Determines critical functions and systems, and the associated durations required for recovery.
- Determines the resources required to support those critical functions and systems, and defines the requirements for a recovery site.
- Identifies the people, skills, resources and suppliers needed to assist in the recovery

## Unit Guide to Disaster Recovery Planning

- process.
- Identifies the vital records, which must be stored offsite to support resumptions of unit operations.
- Documents the appropriate procedures and the information required to recover from a disaster or severe disruption.
- Addresses the need to maintain the currency of the plan's information over time.
- Addresses testing the documented procedures to ensure their completeness and accuracy.

### Objective and Goals for a Disaster Recovery Planning Project

The primary objective of any contingency plan is to ensure the ability of the unit to function effectively in the event of an interruption due to the loss of information, loss of personnel, or loss of access to information and facilities. The goals for disaster planning are to provide for:

- The continuation of critical and important unit operations in the event of an interruption.
- The recovery of normal operations in the event of an interruption.
- The timely notification of appropriate unit and university officials in a predetermined manner as interruption severity or duration escalates.
- The offline backup and availability, or alternative availability, of critical components, including: Data files, Software, Hardware, Voice and Data Communications, Documentation, Supplies and forms, People, Inventory Lists.
- An alternate method for performing activities electronically and/or manually.
- Any required changes in user methods necessary to accomplish such alternate means of processing.
- The periodic testing of the plan to ensure its continuing effectiveness.
- Documentation on the business unit's plan for response, recovery, restoration, and return after severe disruption.

Contingency planning seeks to accomplish the goals above, while minimizing certain exposures to risks that may impact the recovery and business resumption process, including:

- The number of decisions that must be made following a disaster or severe disruption.
- Single point of failure conditions in the unit infrastructure.
- Dependence on the participation of any specific person or group of people in the recovery process.
- The lack of available staff with suitable skills to affect the recovery.
- The need to develop, test, or debug new procedures, programs or systems during recovery.
- The adverse impact of lost data, recognizing that the loss of some transactions may be

inevitable.

## **Conducting the Business Disaster Planning Project**

There are three phases of a Disaster Recovery Planning Project.

- The information needed to identify critical systems, potential impacts and risks, resources, and recovery procedures are gathered in Phase I.
- Phase II is the actual writing and testing of the Disaster Recovery Plan.
- Phase III is ongoing and consists of plan maintenance and audits.

### **I. Information Gathering**

#### **Step One - Organize the Project**

The scope and objectives of the plan and the planning process are determined, a coordinator appointed, the project team is assembled, and a work plan and schedule for completing the initial phases of the project are developed.

#### **Step Two – Conduct Business Impact Analysis**

Critical systems, applications, and business processes are identified and prioritized. Interruption impacts are evaluated and planning assumptions, including the physical scope and duration of the outage, are made.

#### **Step Three – Conduct Risk Assessment**

The physical risks to the unit are defined and quantified. The risks identify the vulnerability of the critical systems, by identifying physical security, backup procedures and/or systems, data security, and the likelihood of a disaster occurring. By definition Risk Assessment is the process of not only identifying, but also minimizing the exposures to certain threats, which an organization may experience. While gathering information for the DRP, system vulnerability is reviewed and a determination made to either accept the risk or make modifications to reduce it.

#### **Step Four - Develop Strategic Outline for Recovery**

Recovery strategies are developed to minimize the impact of an outage. Recovery strategies address how the critical functions, identified in the Business Impact Analysis (step 2), will be recovered and to what level resources will be required, the period in which they will be recovered, and the role central University

## Unit Guide to Disaster Recovery Planning

resources will play in augmenting or assisting unit resources in affecting timely recovery. The recovery process normally consists of these stages:

1. Immediate response
2. Environmental restoration
3. Functional restoration
4. Data synchronization
5. Restoration of business functions
6. Interim site
7. Return home

### **Step Five – Review Onsite and Offsite Backup and Recovery Procedures**

Vital records required for supporting the critical systems, data center operations, and other priority functions as identified in the Business Impact Analysis, are verified and procedures needed to recover them and to reconstruct lost data are developed. In addition, the review of the procedures to establish and maintain offsite backup are completed. Vital records include everything from the libraries, files, and code to forms and documentation.

### **Step Six – Select Alternate Facility**

This item addresses determining recovery center requirements, identifying alternatives and making an alternative facility, site recommendation/selection. Consideration should be given to the use of University resources (e.g., Administrative Information Services, Computer Lab, or another unit) as alternative sites before seeking outside solutions. For further information on alternative University sites please contact the Client Advocacy Office at 517-353-4856.

## **II. Writing and Testing the Plan**

### **Step Seven – Develop Recovery Plan**

This phase centers on documenting the actual recovery plan. This includes documenting the current environment as well as the recovery environment and action plans to follow at the time of a disaster or severe disruption, specifically describing how recovery (as defined in the strategies) for each system and application is accomplished.

### **Step Eight - Test the Plan**

A test plan/strategy for each recovery application as well as the operating environment is developed. Testing occurs on the plans and assumptions made for completeness and accuracy. Modifications occur as necessary following the results of the testing. This portion of the project is perpetual for the life of the plan.

## **III. Maintaining and Auditing the Plan (Ongoing)**

### **Step Nine - Maintain the Plan**

This includes maintaining the plan to keep pace with the changing environment, procedures, and practices.

### **Step Ten – Perform Periodic Audit**

This addresses periodically reviewing the Unit IS Systems Continuity Plan to ensure that it continues to reflect the organization's needs.

## **Project Assumptions to Guide the Development of the Unit's Disaster Recovery Plan**

The following assumptions, coupled with the risk analysis findings, define the boundaries around the planning process. These assumptions will be refined, deleted, or new assumptions added as planning progresses.

- Recovery for anything less than complete destruction will be achievable by using the plan.
- Normally available staff members may be rendered unavailable by a disaster or its aftermath, or may be otherwise unable to participate in the recovery.
- Procedures should be sufficiently detailed so someone other than the person primarily responsible for the work can follow them.
- Recovery of a critical subset (recovery workload) of the unit's critical functions and applications systems during the recovery period will allow the unit to continue critical operations adequately.

## Unit Guide to Disaster Recovery Planning

- A data center disaster may require clients to function with limited automated support and some degradation of service.
- The writing of special purpose programs may be required to enable the client office to effectively return to normal conditions. That is to say clients may need to first rebuild and/or re-enter data that was lost between the time of the last off-site backup and the time of the disaster/disruption; and secondly, enter transactions that accumulate during the period of "no automated support".
- Unit plans typically will not need to deal with power availability. Physical Plant handles this level of planning for the campus. Alternative supply is available from Consumer Energy in the event of a Power Plant failure.
- Unit plans typically will not need to deal with campus-level networking issues.
- Computer Lab handles this level of planning for the campus.

## Step by Step Guide for Disaster Recovery Planning for Michigan State University Units

There is no one best way to write a Disaster Recovery Plan. The following step-by-step guide was created using best practice information, and is intended to help units create their plans as easily and efficiently as possible.

- *The forms and documentation provided in Steps 1 through 6 are to assist each Unit with organizing information needed for developing the Disaster Recovery Plan (DRP). Structure for the plan itself is detailed in Step 7.*
- *These forms, and the planning approach inherent in them, should be modified with information specific to your Unit's daily activities.*
- *If the Unit currently has a Disaster Recovery Plan in place there is no need to recreate it, but the plan should be reviewed to insure the information is complete and current.*

### I. Information Gathering

#### Step One - Organize the Project

*This step would normally be performed by a college dean, chairperson or director, or the senior administrator of the unit, working with the coordinator/project leader identified in Task 1 listed below.*

- Appoint coordinator/project leader, if the leader is not the dean or chairperson.
- Determine most appropriate plan organization for the unit (e.g., single plan at college level or individual plans at unit level)
- Identify and convene planning team and sub-teams as appropriate (for example, lead computer support personnel should be in the team if the plan will involve recovery of digital data and documents).
- At the college and/or unit level set:
  - a. **scope** - *the area covered by the disaster recovery plan, and objectives* - *what is being worked toward and the course of action that the unit intends to follow.*
  - b. **assumptions** - *what is being taken for granted or accepted as true without proof; a supposition: a valid assumption.*
- Set project timetable
- **Draft project plan, including assignment of task responsibilities**
- Obtain Dean's approval of scope, assumptions and project plan, if the leader is not the dean or chairperson.

Sample forms included in the at the end of the document that may be useful in organizing Step One:

- Plan Organization

## Unit Guide to Disaster Recovery Planning

- Project Plan

### Step Two – Conduct Business Impact Analysis

*This step would normally be performed by the coordinator/project leader in conjunction with functional unit administrators (assistant director, associate director, department chair or director).*

In order to complete the business impact analysis, most units will perform the following steps:

- Identify functions, processes and systems
- Interview information systems support personnel
- Interview business unit personnel
- Analyze results to determine critical systems, applications and business processes

Sample forms included in the at the end of the document that may be useful in organizing Step Two:

- **Business Impact Analysis**
- **Critical System Ranking Form**

### Step Three – Conduct Risk Assessment

*The planning team will want to consult with technical and security personnel as appropriate to complete this step. The risk assessment will assist in determining the probability of a critical system becoming severely disrupted and documenting the acceptability of these risks to a unit.*

***For each critical system, application and process as identified in Step:***

1. Review physical security (e.g. secure office, building access off hours, etc.)
2. Review backup systems
3. Review data security
4. Review policies on personnel termination and transfer
5. Identify systems supporting mission critical functions
6. **Identify Vulnerabilities** (Such as flood, tornado, physical attacks, etc.)
7. Assess probability of system failure or disruption
8. Prepare risk and security analysis

Sample forms available for organizing Step Three

- **Security Documentation**
- **Vulnerability Assessment**

## Unit Guide to Disaster Recovery Planning

### Step Four - Develop Strategic Outline for Recovery

*Tasks 1, 2, 3, and 4 below will be mainly applicable to units using or managing technology systems to process critical functions. The coordinator/project leader and the functional unit may wish to appoint the appropriate people (e.g., functional subject matter experts) to perform the subsequent tasks in Step 4.*

1. Assemble **groups** as appropriate for:
  - Hardware and operating systems
  - Communications
  - Applications
  - Facilities
  - Other critical functions and business processes as identified in the Business Impact Analysis
2. For each system/application/process above quantify the following processing requirements:
  - Light, normal and heavy processing days
  - Transaction volumes
  - Dollar volume (if any)
  - Estimated processing time
  - Allowable delay (days, hours, minutes, etc.)
3. Detail all the steps in your workflow for each critical business function (e.g., for student payroll processing each step that must be complete and the order in which to complete them.)
4. Identify systems and applications
  - Component name and technical id (if any)
  - Type (online, batch process, script)
  - Frequency
  - Run time
  - Allowable delay (days, hours, minutes, etc.)
5. Identify vital records (e.g., libraries, processing schedules, procedures, research, advising records, etc.)
  - Name and description
  - Type (e.g., backup, original, master, history, etc.)
  - Where are they stored
  - Source of item or record
  - Can the record be easily replaced from another source (e.g., reference materials)
  - Backup
  - Backup generation frequency
  - Number of backup generations available onsite
  - Number of backup generations available off-site
  - Location of backups

## Unit Guide to Disaster Recovery Planning

- Media type
  - Retention period
  - Rotation cycle
  - Who is authorized to retrieve the backups?
6. Identify if a severe disruption occurred what would be the minimum requirements/replacement needs to perform the critical function during the disruption.
    - Type (e.g. server hardware, software, research materials, etc.)
    - Item name and description
    - Quantity required
    - Location of inventory, alternative, or offsite storage
    - Vendor/supplier
  7. Identify if alternate methods of processing either exist or could be developed, quantifying where possible, impact on processing. (Include manual processes.)
  8. Identify person(s) who supports the system or application
  9. Identify primary person to contact if system or application cannot function as normal
  10. Identify secondary person to contact if system or application cannot function as normal
  11. Identify all vendors associated with the system or application
  12. Document unit strategy during recovery (conceptually how will the unit function?)
  13. Quantify resources required for recovery, by time frame (e.g., 1 pc per day, 3 people per hour, etc.)
  14. Develop and document recovery strategy, including:
    - Priorities for recovering system/function components
    - Recovery schedule

Sample forms available for organizing Step Four

- **Group Assignments**
- **Critical System Processing Requirements for Recovery**

### **Step Five – Review Onsite and Offsite Backup and Recovery Procedures**

*The planning team as identified in Step 1 Task 3 would normally perform this task.*

1. Review current records (OS, Code, System Instructions, documented processes, etc.) requiring protection
2. Review current offsite storage facility or arrange for one
3. Review backup and offsite storage policy or create one
4. Present to unit leader for approval

## Unit Guide to Disaster Recovery Planning

Sample forms available for organizing Step Five

- **Backup and Recovery Procedures**

### Step Six – Select Alternate Facility

*The planning team as identified in Step 1 Task 3 would normally perform this task.*

**ALTERNATE SITE:** *A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster.*

1. Determine resource requirements
2. Assess platform uniqueness of unit systems (e.g., MacIntosh, IBM Compatible, Oracle database, Windows 3.1, etc.)
3. Identify alternative facilities
4. Review cost/benefit
5. Evaluate and make recommendation
6. Present to unit leader for approval
7. Make selection

## II. Plan Development and Testing

### Step Seven – Develop Recovery Plan

*This step would ordinarily be completed by the coordinator/Project Manager working with the planning team.*

Sample forms available for organizing Step Seven

- **Sample Plan Outline**

The steps for developing the Recovery Plan are listed below in outline form to demonstrate how a unit may choose to organize their Disaster Recovery Plan.

#### 1. **Objective**

*The objective may have been documented in the Information Gathering Step 1 "Plan Organization".*

- Establish unit information

#### 2. **Plan Assumptions**

#### 3. **Criteria for invoking the plan**

- Document emergency response procedures to occur during and after an emergency (i.e. ensure evacuation of all individuals, call the fire department, after the emergency check the building before allowing individuals to return)

## Unit Guide to Disaster Recovery Planning

- Document procedures for assessment and declaring a state of emergency
    - Document notification procedures for alerting unit and university officials
    - Document notification procedures for alerting vendors
    - Document notification procedures for alerting unit staff and notifying of alternate work procedures or locations.
  - 4. **Roles Responsibilities and Authority**
    - Identify unit personnel
    - Recovery team description and charge
    - Recovery team staffing
    - Transportation schedules for media and teams
  - 5. **Procedures for operating in contingency mode**
    - Process descriptions
    - Minimum processing requirements
    - Determine categories for vital records
    - Identify location of vital records
    - Identify forms requirements
    - Document critical forms
    - Establish equipment descriptions
    - Document equipment - in the recovery site
    - Document equipment - in the unit
    - Software descriptions
    - Software used in recovery
    - Software used in production
    - Produce logical drawings of communication and data networks in the unit
    - Produce logical drawings of communication and data networks during recovery
    - Vendor list
    - Review vendor restrictions
    - Miscellaneous inventory
    - Communication needs - production
    - Communication needs - in the recovery site
  - 6. **Resource plan for operating in contingency mode**
  - 7. **Criteria for returning to normal operating mode**
  - 8. **Procedures for returning to normal operating mode**
  - 9. **Procedures for recovering lost or damaged data**
  - 10. **Testing and Training**
    - Document Testing Dates
    - Complete disaster/disruption scenarios
    - Develop action plans for each scenario
- [Sample Testing Diagram](#)

## Unit Guide to Disaster Recovery Planning

### 11. Plan Maintenance

- Document Maintenance Review Schedule (yearly, quarterly, etc.)
- Maintenance Review action plans
- Maintenance Review recovery teams
- Maintenance Review team activities
- Maintenance Review/revise tasks
- Maintenance Review/revise documentation

### 12. Appendices for Inclusion

- inventory and report forms
- maintenance forms
- hardware lists and serial numbers
- software lists and license numbers
- contact list for vendors
- contact list for staff with home and work numbers
- contact list for other interfacing departments
- network schematic diagrams
- equipment room floor grid diagrams
- contract and maintenance agreements
- special operating instructions for sensitive equipment
- cellular telephone inventory and agreements

### Step Eight - Test the Plan

1. Develop test strategy
2. Develop test plans
3. Conduct tests
4. Modify the plan as necessary

#### Samples

- Test Plan Strategy
- Test Plan Scenario
- Test Results/Test Evaluation

## III. Ongoing Maintenance

### Step Nine - Maintain the Plan

*Dean/Director/Unit Administrator will be responsible for overseeing this.*

1. Review changes in the environment, technology, and procedures
2. Develop maintenance triggers and procedures

## **Unit Guide to Disaster Recovery Planning**

3. Submit changes for systems development procedures
4. Modify unit change management procedures
5. Produce plan updates and distribute

### **Step Ten – Perform Periodic Audit**

1. Establish periodic review and update procedures

Michigan State University  
[Unit] Project Organization Information

*If the plan will be done at unit level, this information form should be completed for both the college and each unit plan.*

**Project Leader/Coordinator Name:**

**Unit, College, or Department:**

**Scope and Objectives** (The area covered by the disaster recovery plan, what is being worked for, and the course of action that the unit intends to follow): ) :

**Example:**

*The overall objectives of the [Unit] Disaster Recovery Plan (DRP) are to protect University resources and employees, to safeguard the organization's vital records, and to ensure the ability of [Unit] to function effectively in the event of a severe disruption to normal. The primary role of the DRP is to document [Unit]'s plan for response, recovery, restoration, and return after severe disruption.*

*The Plan is a systematic guide from disaster to recovery. The basic approach, general assumptions, and sequence of events that need to be followed will be stated clearly in the documentation that follows. The Plan will be distributed to all key personnel, and they will receive periodic updates. The general approach is to make the plan functional regardless of what type of disaster occurs.*

**Assumptions:** (what is being taken for granted or accepted as true without proof; a supposition: *a valid assumption.*):

**Example:**

- *Recovery for anything less than complete destruction will be achievable by using the plan.*
- *Normally available staff members may be rendered unavailable by a disaster or its aftermath, or may be otherwise unable to participate in the recovery.*
- *Procedures are sufficiently detailed so someone other than the person primarily responsible for the work can follow them.*
- *Plan Organization (e.g. single consolidated plan at college level, each unit will be producing a stand alone plan).*

**Planning Team(s) Contact Info, Roles, and Responsibilities**

**Name:**

**Phone:**

**Preferred email:**

**Role** (e.g., project coordinator/leader, functional contact, lead computer support, etc.):

**Responsibility:**

**Name:**

## Unit Guide to Disaster Recovery Planning

**Phone:**

**Preferred email:**

**Role** (e.g., project coordinator/leader, functional contact, lead computer support, etc.):

**Responsibility:**

**Obtained Management Approval of Scope, Objectives, and Assumptions**

**Manager:**

**Date:**

<b>Sample - Project Plan Information</b>					
<b>Project Milestone</b>	<b>Task</b>	<b>Duration</b>	<b>Start</b>	<b>Finish</b>	<b>Resource</b>
	Organize the Project				
	Appoint coordinator/project leader				
	Obtain management commitment				
	Identify and convene planning team				
	Set scope, assumptions, project milestones				
	Draft project plan, including assignment of task responsibilities				
	Obtain management approval of scope, assumptions and project plan				
	Conduct Business Impact Analysis				
	Identify functions, processes, and systems				
	Interview information systems support personnel				
	Analyze results				
	Prepare impact analysis				
	Conduct Risk Assessment				
	Review physical security				
	Review backup systems				
	Review data security				
	Review policies on personnel termination				
	Identify exposures				
	Prepare risk and security analysis				
	Develop Recovery Strategy				
	Assemble Strategy Teams for each area below				
	Hardware and Operating systems				
	Communications				
	Applications				
	Facilities				
	Other critical functions and business processes as identified in BIA				
	For each system/process quantify processing				
	Light, normal and heavy processing days				
	Transaction volumes				
	Dollar Volume				
	Estimated processing time				
	Allowable delay (hours, days, etc.)				
	Identify process procedures for each				
	Functions				
	Functional Steps				
	Step Activities				
	Identify systems and applications				

**Unit Guide to Disaster Recovery Planning**

<b>Project Milestone</b>	<b>Task</b>	<b>Duration</b>	<b>Start</b>	<b>Finish</b>	<b>Resource</b>
	Component name and technical ID				
	Type (online, batch, manual)				
	Frequency				
	Run Time				
	Allowable delay (hours, days, etc.)				
	Identify Vital Records				
	Name and Description				
	Type (e.g. backup, original, master, history)				
	Source of item or record				
	Generation Frequency				
	Number of generations available off site				
	Media type				
	Number in set (e.g. number of tapes in backup)				
	Retention period				
	Rotation cycle				
	Location				
	Identify minimum processing requirements				
	Type (e.g. server hardware, software, etc.)				
	Item name and description				
	Quantity required				
	Location of inventory, alternatives, etc.				
	Vendor/supplier				
	Identify if alternate methods of processing				
	Identify person(s) who supports the system				
	Identify primary person to contact if system isn't functioning				
	Identify secondary contact				
	Identify all vendors associated with the system or application				
	Document unit strategy during recovery				
	Quantify resources required for recovery				
	Develop and document recovery strategy				
	Priorities				
	Recovery schedule				
	<b>Review Onsite and Offsite Backup and Recovery Procedures</b>				
	Review Current Records (OS, Code, Systems, Procedures, Documentation, etc.) that require protection				
	Review current Offsite storage facility				
	Review backup and offsite storage policy				
	Develop or revise storage facility and backup procedures				
	Select Alternate Facility				

**Unit Guide to Disaster Recovery Planning**

<b>Project Milestone</b>	<b>Task</b>	<b>Duration</b>	<b>Start</b>	<b>Finish</b>	<b>Resource</b>
	Document resource requirements				
	Assess platform uniqueness of unit systems				
	Identify alternatives				
	Review cost/benefit				
	Evaluate and make recommendations				
	Present to unit leader for approval				
	Make selection				
	<b>Develop Recovery Plan</b>				
	Review system documentation				
	Establish unit information				
	Identify unit personnel				
	Recovery team description and charge				
	Recovery team staffing				
	Document procedures for assessment and declaring a state of emergency				
	Document emergency response procedures				
	Document notification procedures for alerting vendors				
	Document notification procedures for University officials				
	Priorities				
	Recovery time constraints				
	Problem escalation requirements				
	Process descriptions				
	Minimum processing requirements				
	Determine categories for vital records				
	Identify location of vital records				
	Identify forms requirements				
	Document critical forms				
	Establish equipment descriptions				
	Document equipment inventory in the unit				
	Document equipment to be used in recovery				
	Produce logical drawings of communications and data networking used in the unit				
	Produce logical drawings of communications and data networking to be used in recovery				
	Software descriptions				
	Software used in production				
	Software used in recovery				
	Vendor list				
	Review vendor restrictions				
	Miscellaneous inventory				

**Unit Guide to Disaster Recovery Planning**

<b>Project Milestone</b>	<b>Task</b>	<b>Duration</b>	<b>Start</b>	<b>Finish</b>	<b>Resource</b>
	Communication needs - production				
	Communication needs - recovery				
	Complete disaster/disruption scenarios				
	Develop action plans for each scenario				
	Review action plans for each scenario				
	Review recovery teams				
	Review team activities				
	Transportation schedules for media and teams				
	Review/revise tasks				
	Review/revise documentation				
	Produce the plan				
	<b>Test the Plan</b>				
	Develop test strategy				
	Develop test plans				
	Conduct tests				
	Modify the plan as necessary				
	<b>Maintain the Plan</b>				
	Review changes in the environment, technology, software, procedures, etc.				
	Develop maintenance triggers and processes				
	Submit changes for systems development				
	Modify unit change management procedure				
	Produce plan updates and distribute				
	<b>Perform Periodic Audits</b>				

## Michigan State University [Unit] Business Impact Analysis Form

The business impact analysis will assist the unit in analyzing all business functions and the effect a disaster may have upon them.

- *One form should be filled out for each function/application.*
- *Review the applications and functions which your area is responsible for, or which are used by your functional area, to determine the support requirements and recovery time frames.*
- *Classify these applications and functions based upon criticality.*

**Department Name:**

**Application** (e.g. SIS, MS Word, Payroll, Training Wizard):

**Function** (e.g., Student Enrollment, Research, Student Employee Hour Input, Class Scheduling):

**What is the purpose of this function or application system?**

**Primary Contact Name for Function:**

**Phone:**

**Secondary Contact for this Function:**

**Phone:**

**How would you classify this function?**

Critical      Essential      Necessary      Desirable

*The categories detail the length of time that an activity can remain disrupted:*

**Critical**      Less than one day

**Essential**      2 - 4 days

**Necessary**      5 -7 days

**Desirable**      More than 10 days

To what extent is this function dependent upon the availability of:

RESOURCE	MODEL AND/OR LOCATION	MAJOR APPLICATION	DEPENDENCY High, Medium, or Low
MSU Mainframe			
Microlab			
Faculty Desktop Computers			
Departmental Server (LAN)			
Building Network			
Telephone - Voice			
MSU Network/Internet Connectivity			
Paper Records			
Network Printing			
Copy Center			
Classroom Technologies and Facility			
Other			

If this function were not performed following a disaster, would there be an impact on the following:

- Human Life
- Federal Funding
- Students
- Operating Efficiency
- Laws Broken
- Reputation

*The chart below is only applicable to those units generating revenue or receiving external funding.*

	Revenue loss if this function were not performed following a disaster	Additional costs to org. if this function were not performed (e.g. fines, lost contracts, federal funding, research grants, etc.)
<b>1 Hour</b>		
<b>1 Day</b>		
<b>2 Days</b>		
<b>3 Days</b>		
<b>1 Week</b>		
<b>1 Month</b>		





**Michigan State University  
[Unit] Vulnerability Analysis Chart**

*A Vulnerability Chart can be completed for a physical location or for each critical system/function. The totals will indicate high areas of vulnerability. The form may be modified to rank vulnerability as high, medium, and low, instead of a numerical ranking system. Using a numerical rating, your most vulnerable areas will be those with the highest total.*

Type of Disaster	Human Impact	Property Impact	Business Impact	Internal Resources	External Resources	Total
	5 High Impact - 1 Low Impact			5 Weak - 1 Strong		
Loss of AC Power						
Loss of Environmental Controls						
Flood						
Tornado						
Fire						
Electrical Storm						
Breaches of Security						
Interruptions of Internal Communications						
Interruptions of External Communications						
System Hang-up or Shutdown						
Degradation of Performance						
Irrational Data Presented to Users						
Files Corrupted or "Lost"						
AC Power Spikes						

Unit Guide to Disaster Recovery Planning

Michigan State University  
[Unit] Subject Matter Expert Groups

Hardware					
Contact Name	Responsibility	Work Phone	email	Cell Phone	Pager
example Jon Doe	LAN Administrator	333-5555	<a href="mailto:doe@msu.edu">doe@msu.edu</a>	555-3333	222-4444
Operating Systems					
Contact Name	Responsibility	Work Phone	email	Cell Phone	Pager
Applications					
Contact Name	Responsibility	Work Phone	email	Cell Phone	Pager
Communications					
Contact Name	Responsibility	Work Phone	email	Cell Phone	Pager
Facilities					
Contact Name	Responsibility	Work Phone	email	Cell Phone	Pager
Other Critical Area					
Contact Name	Responsibility	Work Phone	email	Cell Phone	Pager

**Michigan State University**  
**[Unit] Critical System/Function Processing Requirements**

This form should be filled out for each system and/or function identified as critical in the business impact analysis. It will assist you in analyzing when and how critical function are completed and to determine the steps needed for restoration and recovery.

<b>Critical System/Function:</b>	example Student Payroll Processing
----------------------------------	------------------------------------

**Detail all the steps in your workflow for each critical business function** (e.g., for student payroll processing each step that must be complete and the order in which to complete them.)

Example:

1. Student signs and submits timesheet
2. Supervisor signs and submits timesheet
3. Payroll clerk verifies all forms have been signed and hours documented
4. Payroll clerk fills in the Payroll time report (stutime.xls)
5. Payroll clerk delivers information to Payroll

**Processing Requirements**

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
<b>Light, Normal, or Heavy Processing Day</b>							
<b>Transaction Volume</b>							
<b>Dollar volume (if any)</b>							
<b>Estimated processing time</b>							
<b>Allowable delay (days, hours, minutes, etc.)</b>							

**Systems and Applications Used by this Critical System/Function**

System/Application	Component Name	Tech ID (if any)	Type (online, batch process, script)	Frequency	Runtime	Allowable Delay (Days, Hours, Minutes, etc.)

**Vital Records**

Vital Record	
Type (e.g., backup, original, master, history, etc.)	
Location	
Source of item or record	
Generation frequency	
Number of generations available off-site	
Media type	
Number in set (. e.g., number of tapes in a backup)	
Retention period	
Rotation cycle	
Who is authorized to retrieve the backups?	

*Complete a vital record table for each record identified.*

**Minimum Components Required for Processing**

Component	
Type (e.g., server, software, hardware, etc.)	
Item name and description	
Quantity required	
Location of inventory, alternative, or offsite storage	
Vendor/supplier	

*Complete a component table for each minimum component identified.*

**Identify alternate methods of processing, quantifying where possible, impact on processing. (Include manual processes.)**

**Identify person(s) who supports the system or application**

**Unit Guide to Disaster Recovery Planning**

Support Personnel		Support Personnel	
Name		Name	
Phone		Phone	
Alternate Phone		Alternate Phone	
Pager		Pager	
Title		Title	
Department		Department	
email		email	

**Identify primary and secondary person to contact if system or application cannot function as normal**

Primary Contact		Secondary Contact	
Name		Name	
Phone		Phone	
Alternate Phone		Alternate Phone	
Pager		Pager	
Title		Title	
Department		Department	
email		email	

**Quantify resources required during recovery, by time frame (number of people, computers, servers, etc.)**

Example:  
 2 People each day  
 1 Desktop machine with msunet/internet connectivity  
 1 Printer  
 10 copies of the Student Employee Time Report

**Document unit strategy during recovery (conceptually how will the unit perform?) for this critical system/function:**

Example:  
 During a severe disruption the student payroll process will be handled manually:  
 1. Student hand writes hours, signs and submits  
 2. Supervisor reviews student log  
 3. ....

**Develop and document restoration strategy, including priorities and schedule. The strategy should include all components necessary for the restoration of the system or function:**

**Unit Guide to Disaster Recovery Planning**

**Identify all vendors associated with the system or application**

<b>System/Application/Hardware</b>	<b>Component used in Normal or Alternative Process?</b>	<b>Vendor</b>	<b>Vendor Phone</b>	<b>Vendor Local Contact/Rep</b>	<b>Contingency agreement in place with this vendor?</b>
example Dell Laptop	Normal	Dell		MSU Computer Store	No

**Unit Guide to Disaster Recovery Planning**

**Michigan State University**

**[Unit] Onsite and Offsite Backup and Recovery Procedures**

*Review and document current backup and recovery procedures. If there is a backup policy, but it is not in an offsite location, write the current procedure in the policy section.*

<b>Onsite Backup</b>	<b>Offsite Backup</b>
<p><i>example</i></p> <ul style="list-style-type: none"> <li>• Daily backup of critical files A, B, C and D, via zip drive.</li> <li>• Weekly backup of local directories and files using backup tape.</li> <li>• Daily change dump kept on server rack</li> <li>• Weekly full dump kept on server rack</li> </ul>	<p><i>example</i></p> <ul style="list-style-type: none"> <li>• Daily backup is placed in briefcase and taken home with primary contact nightly.</li> <li>• Weekly backup is stored at Wells Hall in 208. Contact for retrieval.</li> <li>• Weekly full dump copy is stored at Wells Hall in 208.</li> </ul>

*You may want to collaborate with other units/buildings on campus that are located a safe distance away to store each other's backups.*

**Dean/Director Approval**

**Signature:**

**Date:**

*Step 7 Sample Plan Outline*

*This document is a sample only. The plan may be used as a guide, but text must be modified to meet Unit specific Disaster Recovery Procedures.*

**Michigan State University**  
**[Unit]**  
**Disaster Recovery Plan**

**Last Revised 2/7/01**

***EMERGENCY TELEPHONE NUMBERS***

**MSU Police and Public Safety** 355-2221 or 911

**University Physical Plant** 353- 1760

*(Check for “Trouble Truck”)*

**MSU Operator** 0 on Campus 355-1855 Off Campus

**East Lansing Fire, Police, Ambulance** 911

**Computer Center Building Contacts**

Computer Laboratory Lewis H Greenberg Director 220

**353-3390**

Computer Laboratory BC Shift Supervisor Shift Supv 201C

**353-9338 x213**

Computer Laboratory BC Barb Spousta Oper & Prgm Asst Mgr 208

**353-9338**

Computer Laboratory BC Olga Olowolafe Admin Asst II/S 220

**355-3600**

Libraries, Computing & Tech Paul Hunt Vice Provost 400

**353-0722**

***(SHOULD BE REPLACED WITH UNIT’S BUILDING INFORMATION)***

***Objectives of the [Unit] Disaster Recovery Plan***

The overall objectives of the [Unit] Disaster Recovery Plan (DRP) are to protect University resources and employees, to safeguard the organization's vital records, and to ensure the ability of [Unit] to function effectively in the event of a severe disruption to normal operating procedures. The primary role of the DRP is to document [Unit]'s plan for response, recovery, resumption, restoration, and return after severe disruption.

A disaster is defined as the occurrence of any event that causes a significant disruption in [Unit] capabilities. The central theme of the Plan is to minimize the effect a disaster will have upon on-going operations.

The Plan is a systematic guide from disaster to recovery. The basic approach, general assumptions, and sequence of events that need to be followed will be stated in clearly in the documentation that follows. While using the plan during a severe disruption, it may be in the best interest of [Unit] to modify directions for many reasons. All alternative actions should be documented, and as soon as appropriate the plan should be resumed and revisions made as appropriate. The Plan will be distributed to all key personnel, and they will receive periodic updates. The general approach is to make the plan as threat-independent as possible. This means that it should be functional regardless of what type of disaster occurs.

***Assumptions of the [Unit] Disaster Recovery Plan***

1. Recovery for anything less than complete destruction will be achievable by using the plan.
2. Normally available staff members may be rendered unavailable by a disaster or its aftermath, or may be otherwise unable to participate in the recovery.
3. Procedures are sufficiently detailed so someone other than the person primarily responsible for the work can follow them.
4. Recovery of a critical subset (recovery workload) of the unit's critical functions and applications systems during the recovery period will allow the unit to continue critical operations adequately.
5. A disaster may require clients to function with limited automated support and some degradation of service, until full recovery is made.
6. The writing of special purpose programs may be required to enable the client office to effectively return to normal conditions. That is to say clients may need to first rebuild and/or re-enter data that was lost between the time of the last off-site backup and the time of the disaster/disruption; and secondly, enter transactions that accumulate during the period of "no automated support".
7. This plan does not detail campus-level networking issues. The Computer Lab handles this level of planning for the campus.

***Unit Description***

*INSERT HERE: A BRIEF DESCRIPTION OF YOUR UNIT. INCLUDE A GENERAL DESCRIPTION OF THE KIND OF PROCESSING AND SUPPORT MAINTAINED AT YOUR MAIN FACILITY AND ANY PROCESSING AND SUPPORT AT EXTERNAL LOCATIONS.*

***Criteria for Invoking the Disaster Recovery Plan***

The detection of an event which could result in a disaster affecting University Units and information processing systems at Michigan State University is the responsibility of Physical Plant Operations (PPO), Campus Police, Information Systems, or whoever first discovers or receives information about an emergency situation.

As soon as a situation occurs that could result in a severe disruption to service, the on-site personnel should contact the appropriate emergency authorities and then take the necessary steps to minimize property damage and injury to people in the vicinity. The following people must be notified:

- Normally, Physical Plant Operations and /or the Campus Police receive the initial notice through their alarm monitoring capabilities. If the problem does not activate a normal alarm system, immediately notify these two areas.
- [Unit] Building Contacts
- Once the appropriate authorities and building contacts have been notified, contact the [Unit] Disaster Recovery Project Leader so that the team can personally make an on-site evaluation of the disaster.
- The Operations and Systems Primary and Secondary Contacts will be contacted by the Project Leader/Coordinator and/or their designees as appropriate.

**MSU Police and Public Safety** **355-2221 or 911**

**University Physical Plant** **353- 1760**

**East Lansing Fire, Police, Ambulance** **911**

**Computer Center Building Contacts** ***(REPLACE WITH UNIT'S INFORMATION)***

Computer Laboratory Lewis H Greenberg Director 220 **3-3390**

Computer Laboratory BC Shift Supervisor Shift Supv 201C **3-9338 x213**

Computer Laboratory BC Barb Spousta Oper & Prgm Asst Mgr 208 **3-9338**

Computer Laboratory BC Olga Olowolafe Admin Asst II/S 220 **5-3600**

Libraries, Computing & Tech Paul Hunt Vice Provost 400 **3-0722**

*(Include Information from Step 1 – Planning Team if appropriate)*

**Disaster Recovery Team(s) Contact Info, Roles, and Responsibilities**

**Name:**  
**Phone:**  
**Preferred email:**  
**Role:**  
**Responsibility:**

**Name:**  
**Phone:**  
**Preferred email:**  
**Role:**  
**Responsibility:**

**Name:**  
**Phone:**  
**Preferred email:**  
**Role:**  
**Responsibility:**

The Disaster Recovery Management team will personally visit the site and make an initial determination of the extent of the damage. Based on their assessment, all or part of the [Unit] Disaster Recovery Plan will be initiated. The team will decide:

1. If normal operations can be continued at the site and repairs can be started as soon as possible.
  - Minor Damage—Processing can be restarted in a short time with no special recall of personnel.
  - Anticipated downtime is less than one day.
  - Damage could be to hardware, software, mechanical equipment, electrical equipment, or the facility.
2. If normal operations can be continued or restarted with the assistance of only certain recovery teams.
  - Major Damage— Selected teams will be called to direct restoration of normal operations at current site.
  - Estimated downtime is two to six days.
  - Major damage to hardware or facility.

**Unit Guide to Disaster Recovery Planning**

3. If limited operations can be continued at the site and plans started to repair or replace unusable equipment.
4. If the facility is destroyed to the extent that an alternate facility must be used.
  - Catastrophe— Damage is extensive.
  - Restoration will take upwards from one week.
  - Computer room or facility could be completely destroyed.
  - All team leaders will be called to begin a total implementation of the [Unit] Contingency Plan.
5. The extent that the [Unit] Disaster Recovery Plan(s) must be initiated.
6. The Management Team will decide on its plan of action and then notify senior management.
7. If the action plan requires the assistance of other recovery teams, those teams will be notified.

**Roles Responsibilities and Authority**

If a determination is made to notify all other teams, the Disaster Recovery Project Team will phone each Group Leader. A brief message will be dictated over the phone and the called person will write down the message. At the end of the message, the called person will read back the message to verify that all critical information is stated.

<b>Hardware</b>					
Resource Name	Responsibility	Work Phone	Hm Phone	Cell Phone	Pager
<b>Operating Systems</b>					
Resource Name	Responsibility	Work Phone	Hm Phone	Cell Phone	Pager
<b>Applications</b>					
Resource Name	Responsibility	Work Phone	Hm Phone	Cell Phone	Pager
<b>Communications</b>					
Resource Name	Responsibility	Work Phone	Hm Phone	Cell Phone	Pager
<b>Other Critical Area</b>					
Resource Name	Responsibility	Work Phone	Hm Phone	Cell Phone	Pager

**Unit Guide to Disaster Recovery Planning**

The Group Leaders will then use the same procedure to contact other team members in the list above and the Primary and Secondary System/Function contacts as identified in the Critical System Process Information (*this information was gathered in forms in the Information Gathering Phase Step 4 item 9 and 10*).

Primary Contact		Secondary Contact	
Name		Name	
Phone		Phone	
Alternate Phone		Alternate Phone	
Pager		Pager	
Title		Title	
Department		Department	

The Primary and Secondary contacts will then use the same procedure to contact the support staff.

Support Personnel		Support Personnel	
Name		Name	
Phone		Phone	
Alternate Phone		Alternate Phone	
Pager		Pager	
Title		Title	
Department		Department	
email		email	

**Procedures for operating in contingency mode**

*These procedures were documented in Step 4 using the Critical System Processing Information Form. Types of Information that would be included in this section:*

- Process descriptions
- Minimum processing requirements
- Determine categories for vital records
- Identify location of vital records
- Identify forms requirements
- Document critical forms
- Establish equipment descriptions
- Document equipment - in the recovery site
- Document equipment - in the unit
- Software descriptions
- Software used in recovery
- Software used in production

## Unit Guide to Disaster Recovery Planning

- Produce logical drawings of communication and data networks in the unit
- Produce logical drawings of communication and data networks during recovery
- Communication needs - production
- Communication needs - in the recovery site
- Disable certain processes, functions, or sub-systems
- Use of alternative "Office Automation" functions to perform mission Word processors, spreadsheets, copy machines, fax machines, etc.
- Shift or call in personnel as needed to support the mission
- Shift communications channels to alternates as needed
- Transfer function/mission to different organization/system/contracting

### Resource plan for operating in contingency mode

#### Criteria for returning to normal operating mode

The [Unit] criteria for returning to normal operating mode is detailed below.

- Establish criteria for returning to normal operations

#### Procedures for returning to normal operating mode

The [Unit] disaster recovery/restoration procedures for Mission Critical Processes are:

- Procedures to procure replacement equipment and supplies as necessary
- Procedures to restore/restart systems as required
- Procedures to check system functions/results
- Procedures for notifying personnel to return to normal operating mode

#### Procedures for recovering lost or damaged data

- Procedures to correct and restore corrupt/lost data

### Testing and Training

*Document Test Strategy, which will be detailed and performed in Step 8. The strategy should include dates, resources that will be managing and performing testing, and an appendix to the actual testing scenarios.*

### Plan Maintenance

Ensuring that the Plan reflects ongoing changes to resources is crucial. This task includes updating the Plan and revising this document to reflect updates; testing the updated Plan; and training personnel. The Business Continuity Management Team Coordinators are responsible for this comprehensive maintenance task.

Quarterly, the Disaster Recovery Planning Project Coordinator/Leader ensures that the Plan undergoes a more formal review to confirm the incorporation of all changes since the prior

**Unit Guide to Disaster Recovery Planning**

quarter. Annually, the Disaster Recovery Planning Project Coordinator/Leader initiates a complete review of the Plan, which could result in major revisions to this document. These revisions will be distributed to all authorized personnel, who exchange their old plans for the newly revised plans. At that time the Coordinators will provide an annual status report on disaster recovery planning to the Dean/Chairperson of [Unit College/Department].

**Maintenance Review recovery teams**

*The personnel responsible for performing plan maintenance should be documented here.*

**Maintenance Cycle and Triggers**

The [Unit] Disaster Recovery Plan will be reviewed and updated on an annual basis in conjunction with the plan testing.

In addition, the disaster recovery plan will be maintained if any changes to the operating environment occur, such as:

- Facility changes
- Equipment changes
- Major changes to existing applications
- Off site storage location changes
- New software upgrades or installs
- Changes to backup procedures
- Changes to key personnel identified in the document

**Maintenance Record**

The purpose of this section is to provide an ongoing record of the changes, which have been made to the [Unit] Disaster Recovery Plan.

Updated	Reason for Update	Comments

**Plan Distribution**

The plan will be redistributed in the event that changes occur according to the list below.

**PLAN DISTRIBUTION MATRIX**

<b>Organization</b>	<b>Recipient</b>	<b>Location</b>	<b># of Copies</b>
Disaster Recovery Planning Teams			
Building Contacts			
Audit Division			
Campus Police			
AIS Operations and Systems			
CAO			
Physical Plant			
President's Office			
Primary System/Function Contacts			
Recovery Personnel			

**Appendices for Inclusion**

- inventory and report forms
- maintenance forms
- hardware lists and serial numbers
- software lists and license numbers
- contact list for vendors
- contact list for staff with home and work numbers
- contact list for other interfacing departments
- network schematic diagrams
- equipment room floor grid diagrams
- contract and maintenance agreements
- special operating instructions for sensitive equipment
- cellular telephone inventory and agreements
- other documentation needed in the event of a severe disruption
- Test scenarios

**Michigan State University  
[Unit] Test Strategy Document**

*The DRP Test Strategy Document is a high level description of the overall means by which the disaster recovery plans for the critical functions, processes or systems of the unit will be exercised to determine the efficacy of the plan, and the need to remediate either the plan itself, or, the means by which the plan is going to be carried out.*

***The Strategy Document should contain the following components:***

- Unit/Department that will be covered in testing
- Critical functions/processes/systems to be covered in testing
- Objectives to be achieved by the tests
- Types of tests to be conducted (see SAMPLE Test Plan Scenario Document for explanation of test types), and high level description of scenarios.
- Persons/teams involved in testing
- Frequency and time frames for testing
- Desired effect of test results in evaluating the DRP
- Plans for maintaining the plan subsequent to testing

## Michigan State University [Unit]Test Plan/Scenario Document

*Individual test plans or scenarios arise out of the overall DRP testing strategy for the unit. They are generally written at the function/process/specific system level. There are five different types of tests that may be run. Each is appropriate for the objectives to be achieved and the type of process being tested. The five types are:*

**Table Top Test:** the most informal disaster recovery testing procedure. Each disaster recovery team verbally reviews the processes to recover data and applications.

**Walk-Through:** more in-depth discussions about the actual steps in the recovery process. Members of each team use the disaster recovery plan to discuss the backup process and how to execute each step.

**Simulation Exercise:** a more advanced test. A simulation uses the existing disaster recovery plan to measure its effectiveness against a fictional series of calamitous events. All of the responsible staff must be present at the simulation, with each business or IS unit sending their respective disaster recovery teams to the event as well.

**Alternate Site:** If you use alternate facilities for hosting data centers or storage, you should perform this test in order to ensure the alternate site operates correctly during the recovery process.

**Automated tests:** require very little interaction from team and staff members and can be used on an ongoing basis to test the operations of applications. These tests involve robotic monitoring systems. The system performs queries on software and applications on a regular basis to determine their operational status.

**Unit/Department Name:**

**Critical Function/Process:**

*From the Business Impact Analysis and Recovery Strategy, indicate the function/process or system having a disaster recovery strategy which requires testing.*

**Objectives to Be Achieved by this Test:**

*In keeping with the recovery strategy, what do you hope to achieve with this test.*

**Scenario(s) For Carrying Out The Objectives Of This Test:**

*Identify the type of test you will be using, and how it will be carried out. It may be best to break*

*this down into a series of steps (the results of which will be documented in the "Test Evaluation" form).*

**Frequency & Dates for the Test:**

*Identify the frequency (i.e., yearly, monthly, etc.), and the specific time frames (month/days) for carrying out the test.*

**Responsible Parties:**

Identify the person(s) who is(are) responsible for:

- writing the detailed plan for the test (if necessary)
- supervising the execution of the test
- providing/securing resources for the test
- documenting the results of the test
- updating the plan as a result of the test

## Michigan State University [Unit] Test Results/Test Evaluation Document

*For the objectives for each test plan/scenario, document the results of the test; determine if it was successful in light of the specific test objectives, and overall objectives for your DRP. Determine if the DRP requires modification, or, if DRP measures require adjustment.*

**From the Test Plan for this Function/Process/System, extract the following: Critical function/process; objectives to be achieved by test; scenario steps.**

**Critical Function/Process:**

**Step:**

**Result:**

**Step:**

**Result:**

**Step:**

**Result:**

**Test Evaluation:** *(Were the test objectives met at a level which was: Successful, no modification to plan required; Successful, but plan should be modified; Unsuccessful; etc.)*

**Recommended Action (based on test evaluation):**

*Document what remedial action should be taken: E.g., correct what went wrong during the test; correct the DRP; etc.*

**Action Taken:**

Document what action was/will be taken, by whom, and when.